Google Inc. et al v. Egger et al Doc. 545

GREGORY G. KATSAS
Assistant Attorney General, Civil Division
JOHN C. O'QUINN
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
ALEXANDER K. HAAS
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782—Fax: (202) 616-8460

Attorneys for the Government Defendants

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Solely Relates To: *Al-Haramain Islamic Foundation* *et* *al.* *v. Bush*, *et* *al.* (07-CV-109-VRW)	No. M:06-CV-01791-VRW **DECLARATION OF ARIANE E. CERLENKO, NATIONAL SECURITY AGENCY, IN SUPPORT OF DEFENDANTS' MOTION FOR A STAY PENDING APPEAL AND FOR CERTIFICATION OF AN INTERLOCUTORY APPEAL** Honorable Vaughn R. Walker

I, Ariane E. Cerlenko, do hereby state and declare as follows:

1. I am the Associate General Counsel for Litigation in the Office of General Counsel for the National Security Agency (NSA). The Office of General Counsel ("OGC") is responsible for providing legal services to the Director of the NSA and to all subordinate NSA officials and elements. I oversee a staff of fifteen (15) attorneys, paralegals, and office support personnel. I have served in this position since July 2003, first in an acting capacity and, since September 2004, as the permanent head. Prior to that time, I served as the Assistant General

Dockets.Justia.com

Counsel of Civil Litigation from July 2000 to July 2003, where I was primarily responsible for the conduct of civil litigation matters for the NSA.

2. In my capacity as the Associate General Counsel for the Litigation Division, I am responsible for oversight of NSA involvement in all civil and criminal litigation matters. I have been responsible for the NSA's oversight of this litigation since its inception, working directly with Department of Justice litigation counsel and supervising attorneys in the OGC who are assisting in this matter. I have reviewed the content of public and classified declarations filed by NSA officials in this action, including by the Director of the NSA, Lt. Gen. Keith Alexander. I also have read the Court's Order of January 5, 2009. The purpose of this declaration is to summarize the process under which an individual may be granted access to classified NSA information. As set forth below, under these procedures, even if a person is found to be suitable to receive access to classified information, the agency that originates classified information would retain authority to make a separate determination on whether that person has a "need to know" and may in fact be granted access to its classified information. In addition, subsequent to the Court's January 5, 2009 Order, the NSA Director has reviewed the matter and has determined that the plaintiffs' counsel do not have the requisite "need to now" and therefore should not receive access to the NSA information at issue in this case.

A. Security Clearance and Access Process

3. The President of the United States, through the authority vested in him by the Constitution and the laws of the United States, has prescribed procedures governing access to classified information. Specifically, through Executive Orders issued by the President, a uniform system of classifying, safeguarding, and declassifying national security information has been created. *See* Exec. Order No. 12,958, 60 Fed. Reg. 19825 (Apr. 17, 1995), as amended by Exec. Order No. 13,292, 68 Fed. Reg. 15315 (Mar. 25, 2003); *see also* Exec. Order 12,968, 60 Fed. Reg. 40,245 (Aug. 2, 1995) (establishing a uniform Federal personnel security program for employees who will be considered for access to classified information).

4. Pursuant to the Executive Order, all applicants seeking access to classified NSA

information must complete a two-step process. *See* Exec. Ord. 12958 § 4.1. One step is that a person must receive a favorable determination of eligibility for access to classified information. *Id.* at § 4.1(a)(1). This is also referred to as a "suitability" determination. In this case, the process for determining the suitability of plaintiffs' counsel to receive classified information would be overseen by officials with the United States Department of Justice who are responsible for ensuring the security of classified information in court proceedings. After a background investigation, DOJ security officials would determine if plaintiffs' counsel are eligible for a security clearance at a particular level (*i.e.*, Confidential, Secret, or Top Secret). *See* Exec. Ord. 12958, § 1.2 (describing levels of clearances).

5. A favorable eligibility or "suitability" determination, and the granting of a security clearance, does not mean that a person may receive access to classified information, but only that they are eligible to receive such information. In order to receive actual access to classified information, separate approval by the Executive Branch department or agency that controls the information is also necessary. Specifically, the originating agency must separately determine whether an individual has a "need to know" certain classified information. *See* Exec. Ord. 12958 §§ 4.1(a)(3). A "need to know" classified information is defined as "a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." *See* Exec. Ord. 12958 § 6.1(z).

6. In addition, if the information at issue resides in a "special access program," access is further restricted and may only be granted in accordance with the procedures established by an agency head. *See* Exec. Ord. 12958 § 4.3. The Executive Order provides that the number of persons who will have access to special access programs "will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved." *Id.* § 4.3(b)(3). In addition, the Director of National Intelligence ("DNI") has promulgated an Intelligence Community (IC) Directive that concerns special access programs that govern access to particularly sensitive information concerning intelligence related matters

referred to as "Sensitive Compartmented Information" ("SCI"). *See* ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" (Attachment A). Under ICD 704, "the DNI retains the authority in any case to make a determination granting or denying access" to SCI information and "all such determinations are discretionary and based on [Intelligence Community] mission requirements, and do not create any rights, substantive or procedural." *Id.* at 1-2.

7. If the NSA decides to grant access to classified NSA information, the individual obtaining access must first undergo an orientation process (known as a "read in"). The purpose of the read in process is to describe facts concerning the compartmented activity so that the person being granted access is generally familiar with the nature of the classified information in the compartment, why that information is classified, the harm to national security that would result from disclosure of information contained in the compartment, and the specialized handling and storage restrictions and any additional requirements that apply to information in the compartment. Thus, the read in process itself entails the disclosure of classified information. Access to information residing in the compartment cannot occur prior to the "read in" described above. In addition, even after an individual has been "read in" to a particular program, NSA continues to control the particular information provided to that individual based upon the individual's need to know.

B. Access to NSA Information in this Case

8. In this case, the NSA decided to provide classified information directly to the Court for *ex parte*, *in camera* review in connection with the state secrets privilege assertion made by the DNI in this case. These submissions set forth classified information related to the functions and activities of NSA and were classified at the TOP SECRET/SCI level and contain information concerning the Terrorist Surveillance Program, which is an NSA special access program. This information was not intended to be shared with the plaintiffs' counsel, but to assist the Court in deciding the Government's state secrets privilege assertion.

9. Under the particular circumstances of this case, even if plaintiffs' counsel were to obtain a favorable suitability determination, the NSA Director has determined that neither plaintiffs nor their counsel have a need for access to classified NSA information that has been (or would be) excluded under the state secrets privilege assertion. This includes: the sealed document inadvertently disclosed by the Treasury Department in 2004, the fact of whether or not the plaintiffs have been subject to surveillance by the NSA under any authority, and any information concerning the operations of the Terrorist Surveillance Program authorized by the President after the 9/11 attacks. As indicated in the Government's state secrets privilege assertion, NSA has determined that the disclosure of this information would cause exceptional harm to national security. *See* Public and Classified Declarations of Lt. Gen. Keith Alexander, Director of the NSA filed in this action. The NSA Director has further determined that it does not serve a governmental function, within the meaning of the Executive Order, to disclose the classified NSA information at issue in this case simply to assist the plaintiffs' counsel in representing the interests of private parties who have filed suit against the NSA and who seek to obtain disclosure of information related to NSA intelligence sources and methods.

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed this the 19th day of January 2009.

ARIANE E. CERLENKO

INTELLIGENCE COMMUNITY DIRECTIVE
NUMBER 704

PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION AND OTHER CONTROLLED ACCESS PROGRAM INFORMATION

(EFFECTIVE: 01 OCTOBER 2008)

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002, as amended; Executive Order (EO) 12333, as amended; EO 12958, as amended; EO 12968, EO 13467, and other applicable provisions of law.

B. PURPOSE: This Intelligence Community Directive (ICD) establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs. This directive also documents the responsibility of the DNI for overseeing the program producing these eligibility determinations. It directs application of uniform personnel security standards and procedures to facilitate effective initial vetting, continuing personnel security evaluation, and reciprocity throughout the Intelligence Community (IC). This directive rescinds Director of Central Intelligence Directive 6/4, 02 July 1998, as amended; Intelligence Community Policy Memorandum (ICPM) 2006-700-3, 12 July 2006; ICPM 2006-700-4, 12 July 2006; ICPM 2006-700-5, 12 July 2006; and ICPM 2006-700-6, 12 July 2006.

C. APPLICABILITY: This directive applies to the IC, as defined by the National Security Act of 1947, as amended; and other departments or agencies that may be designated by the President, or designated jointly by the DNI, and the head of the department or agency concerned, as an element of the IC or those government entities designated to determine eligibility for SCI access.

D. POLICY

1. The DNI establishes eligibility standards for access to SCI and other controlled access program information. The DNI delegates to Heads of IC Elements the authority to grant access to such information in accordance with this directive. Heads of IC Elements may further delegate determination approval authority to the Cognizant Security Authority (CSA). Notwithstanding this delegation, the DNI retains the authority in any case to make a determination granting or denying access to such information. All such determinations are

discretionary and based on IC mission requirements, and do not create any rights, substantive or procedural.

2. In all access determinations, national security must be protected. Exceptions to the personnel security standards in this directive shall be based on a finding that the risk to national security is manageable and acceptable. Nothing in this directive, or its accompanying procedural guidelines, shall preclude the DNI, or Principal Deputy DNI, in consultation with the relevant Head of an IC Element, from taking actions regarding a subject's access to SCI and other controlled access information.

3. IC elements using polygraph programs for personnel security purposes may require polygraph examinations when the Head of an IC Element deems it to be in the interest of national security. These polygraph programs shall include standardized training and certification of operators to ensure consistent and fair processes.

4. Heads of IC Elements or designees may determine that it is in the national interest to authorize temporary access to SCI and other controlled access program information, subject to the following requirements -- temporary access approvals shall be granted only during national emergencies, hostilities involving United States personnel, or in exceptional circumstances when official functions must be performed, pursuant to EO 12968. Temporary access approvals shall remain valid until the emergency(ies), hostilities, or exceptional circumstances have abated or the access is rescinded. In any case, temporary access shall not exceed one year.

5. When eligibility for access is first adjudicated, CSAs are required to use sound risk management. Continuous personnel security and counterintelligence (CI) evaluation will be required of all personnel granted access to SCI and other controlled access program information.

6. Subjects who have immediate family members or other persons who are non-United States citizens to whom the subject is bound by affection or obligation may be eligible for access to SCI and other controlled access program information as the result of a condition, deviation, or waiver from personnel security standards.

7. This ICD and its associated Intelligence Community Policy Guidance (ICPG) promulgate the personnel security policy of the DNI. These associated ICPGs are described below:

a. The evolving critical threat environment requires that innovative security, CI, and risk management measures be continually developed and implemented to support intelligence production, information sharing, reciprocity, and personnel mobility. Eligibility for access to SCI and other controlled access program information shall be contingent on meeting DNI personnel security standards as measured by investigative activities prescribed in ICPG 704.1 and the application of specific adjudicative guidelines contained in ICPG 704.2.

b. Guidance pertaining to denial of initial access to SCI and other controlled access programs or revocation of continued access eligibility, and the appeals process for such actions is contained in ICPG 704.3.

c. All IC security elements shall accept in-scope personnel security investigations and access eligibility determinations that are void of conditions, deviations or waivers. Specific guidelines are contained in ICPG 704.4.

d. The IC Scattered Castles repository, or successor database, shall be the authoritative source for personnel security access approval verifications regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards. Heads of IC Elements shall ensure that accurate, comprehensive, relevant, and timely data are delivered to this repository. Specific guidelines are contained in ICPG 704.5.

e. Additional ICPGs, and amendments to the ICPGs listed above, may be promulgated by the Deputy Director of National Intelligence for Policy, Plans, and Requirements (DDNI/PPR) following formal IC coordination.

E. PERSONNEL SECURITY STANDARDS

Threshold criteria for eligibility for access to SCI are as follows:

1. The subject requiring access to SCI must be a U.S. citizen.

2. The subject must be stable, trustworthy, reliable, discreet, of excellent character, and sound judgment; and must be unquestionably loyal to the United States.

3. Members of the subject's immediate family and any other person(s) to whom the subject is bound by affection or obligation shall not be subject to physical, mental, or other forms of duress by either a foreign power or by persons who may be or have been engaged in criminal activity, or who advocate either the use of force or violence to overthrow the U.S. Government, or alteration of the form of the U.S. Government by unconstitutional means.

F. EXCEPTIONS TO PERSONNEL SECURITY STANDARDS

1. A Head of an IC Element may grant access based on a condition, deviation, or waiver to the above standards based on all available information that the specific risk to national security is manageable and acceptable. In such cases, additional personnel security and/or CI evaluation may be required. All risk assessments shall become a part of an individual's security file and the results of the risk assessment shall be annotated as an exception in the record.

2. The DNI, or designee, is the exclusive authority for granting an exception to the requirement that the subject be a U.S. citizen. Exceptions to this requirement shall require a letter of compelling need that is based upon specific national security considerations.

3. When an exception to these personnel security standards is warranted and a subject is granted access to SCI and other controlled access program information, the approving organization shall document its findings in the subject's security record and the Scattered Castles or successor database. The findings shall be characterized as a waiver, condition, or deviation.

G. RESPONSIBILITIES

1. **Deputy Director of National Intelligence for Policy, Plans, and Requirements** is responsible for enforcing the authorities and carrying out the responsibilities of the DNI with respect to security.

2. **Assistant Deputy Director of National Intelligence for Security** is responsible for overseeing IC security programs.

3. **Director of the DNI Special Security Center** is responsible for developing, coordinating, and implementing DNI security policies throughout the IC and providing IC security services in the form of research, training, and security databases.

4. **Heads of IC Elements** are responsible for uniformly and consistently implementing DNI security policies governing access to classified national intelligence.

5. **Cognizant Security Authority** is responsible, as the senior security authority designated by a Head of an IC Element, for overseeing all aspects of security program management within an organization. The CSAs may formally delegate responsibility for certain security matters to specific elements within their agencies.

H. EFFECTIVE DATE: This ICD is effective on the date of signature.

JM McConnell
Director of National Intelligence

1 OCT 08
Date

APPENDIX A – ACRONYMS

ICD 704 -- PERSONNEL SECURITY STANDARDS AND PROCEDURES GOVERNING ELIGIBILITY FOR ACCESS TO SENSITIVE COMPARTMENTED INFORMATION AND OTHER CONTROLLED ACCESS PROGRAM INFORMATION

CI	counterintelligence
CSA	Cognizant Security Authority
DNI	Director of National Intelligence
EO	Executive Order
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
ICPM	Intelligence Community Policy Memorandum
SCI	Sensitive Compartmented Information
US	United States